(12)特許協力条約に基づいて公開された国際出願

(19) 世界知的所有権機関
国際事務局

(43) 国際公開日
2003年12月24日 (24.12.2003)

PCT

(10) 国際公開番号
WO 03/107263 A1

(51) 国際特許分類[7]: G06K 17/00, G06F 17/60

(21) 国際出願番号: PCT/JP03/07560

(22) 国際出願日: 2003年6月13日 (13.06.2003)

(25) 国際出願の言語: 日本語

(26) 国際公開の言語: 日本語

(30) 優先権データ:
特願2002-174991 2002年6月14日 (14.06.2002) JP

(71) 出願人 (米国を除く全ての指定国について): 株式会社ジェーシービー (JCB CO., LTD.) [JP/JP]; 〒107-8686 東京都 港区 南青山五丁目１番２２号 Tokyo (JP).

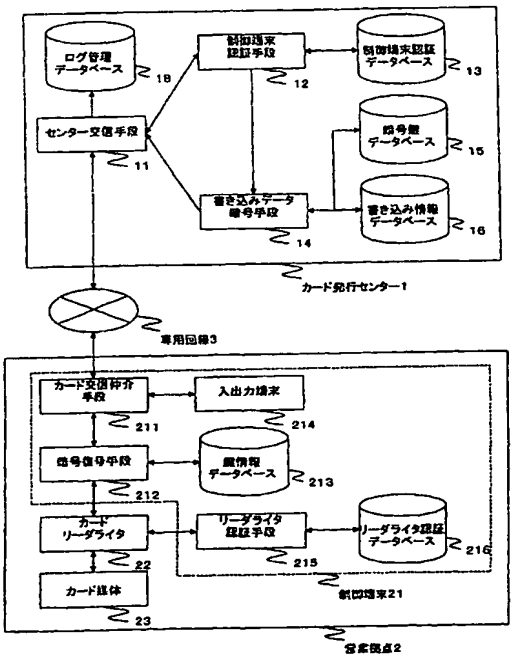
(72) 発明者; および
(75) 発明者/出願人 (米国についてのみ): 川本 昌由 (KAWAMOTO,Masayoshi) [JP/JP]; 〒107-8686 東京都 港区 南青山五丁目１番２２号 株式会社ジェーシービー 会員サービス部内 Tokyo (JP). 入山 弘滋 (IRIYAMA,Hiroshige) [JP/JP]; 〒107-8686 東京都 港区 南青山五丁目１番２２号 株式会社ジェーシービー システム部内 Tokyo (JP). 松山 永徳 (MATSUYAMA,Hisanori) [JP/JP]; 〒107-8686 東京都 港区 南青山五丁目１番２２号 株式会社ジェーシービー情報ネットワーク部内 Tokyo (JP).

(74) 代理人: 名越 秀夫, 外 (NAKOSHI,Hideo et al.); 〒150-0001 東京都 渋谷区 神宮前３丁目７番５号 青山ＭＳビル７階 生田・名越法律特許事務所 Tokyo (JP).

[続葉有]

(54) Title: CARD ISSUING SYSTEM AND CARD ISSUING METHOD

(54) 発明の名称: カード発券システム及びカード発券方法



18...LOG MANAGEMENT DATABASE
11...CENTER COMMUNICATION MEANS
12...CONTROL TERMINAL AUTHENTICATION MEANS
14...WRITTEN-DATA ENCRYPTION MEANS
13...CONTROL TERMINAL NON-AUTHENTICATION DATABASE
15...ENCRYPTED-KEY DATABASE
16...WRITTEN-INFORMATION DATABASE
1...CARD ISSUE CENTER
3...DEDICATED LINE
211...CARD COMMUNICATION INTERMEDIATE MEANS
212...DECRYPTION MEANS
22...CARD READER/WRITER
23...CARD MEDIUM
214...INPUT/OUTPUT TERMINAL
213...KEY INFORMATION DATABASE
215...READER/WRITER AUTHENTICATION MEANS
216...READER/WRITER AUTHENTICATION DATABASE
21...CONTROL TERMINAL
2...SERVICE LOCATION

(57) Abstract: In order to issue, in real time, an IC card, which includes personal information of a client, with a security maintained, at that service location of a card issue company which is in any one of security environments, a card issue center (1) has center communication means (11) for transmitting the written-in-card data of the client to a service location (2), while the service location (2) has card communication intermediate means (211) that receives the written-in-card data from the center communication means (11) to transfer them, without storing them in a terminal (21) of the service location (2), directly to an IC card medium (23) connected to the terminal (21).

[続葉有]

WO 03/107263 A1

(81) 指定国 (国内): AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DZ, EC, EE, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NI, NO, NZ, OM, PH, PL, PT, RO, RU, SC, SD, SE, SG, SK, SL, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, YU, ZA, ZM, ZW.

(84) 指定国 (広域): ARIPO 特許 (GH, GM, KE, LS, MW, MZ, SD, SL, SZ, TZ, UG, ZM, ZW), ユーラシア特許 (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), ヨーロッパ特許 (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HU, IE, IT, LU, MC, NL, PT, SE, SI, SK, TR), OAPI 特許 (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

規則4.17に規定する申立て:
— すべての指定国のための不利にならない開示又は新規性喪失の例外に関する申立て (規則4.17(v))

添付公開書類:
— 国際調査報告書
— 不利にならない開示又は新規性喪失の例外に関する申立て

2文字コード及び他の略語については、定期発行される各PCTガゼットの巻頭に掲載されている「コードと略語のガイダンスノート」を参照。

(57) 要約: 顧客の個人情報を内蔵するＩＣカードをいかなるセキュリティ環境下にあるカード会社の拠点に於いても、セキュリティを確保し且つリアルタイムで発券するため、カード発行センター１は、顧客のカード書き込みデータを拠点２に送信するセンター交信手段１１を有し、拠点２は、センター交信手段１１からカード書き込みデータを受信し、拠点２の端末２１内に蓄積することなく端末２１と接続されたＩＣカード媒体２３に直接転送するカード交信仲介手段２１１を有する。

明　細　書

カード発券システム及びカード発券方法

技術分野

本発明は、個人情報を内蔵するＩＣカードをいかなるセキュリティ環境下にあるカード会社の拠点に於いても、セキュリティを確保し且つリアルタイムで発券するカード発券システム及びカード発券方法に関するものである。

背景技術

近年、ＩＣカードが普及している。ＩＣカードとは、内蔵された集積回路に、カード番号等の固有情報や個人情報やカード用途に応じたアプリケーションプログラムを書き込んだカードであり、クレジットカードやポイントカードや交通機関の運賃カード等の複数の様々な用途に利用可能である。ＩＣカードに書き込まれる情報は暗号化されている為、磁気カードやプラスチックカードに比べて偽造が困難であり、固有情報や個人情報のセキュリティが確保されるというメリットがある。

従来、カード会社等で発行されるＩＣカードの発券処理は、ＩＣカード自体に固有情報や個人情報等を書き込まなければならない為、高度なセキュリティ環境下に置かれたカード会社のカード発行センターに於いて行われることが主流であったが、この場合、ＩＣカードを顧客に発行するまでに時間や輸送コストがかかり、又輸送の際のセキュリティにも気を付けなければならないという問題があった。

そこで、各所にあるカード会社の営業拠点に於いてＩＣカードの発券を行い、顧客のカード申込みからカード発行までの時間を短縮したシステムが、特開２００１－２６６０７６号公開公報に開示されている。

又、従来、ＩＣカードの発券を営業拠点に於いて行う場合は第３図に示すように、営業拠点２ａの制御端末２１ａは、ＩＣカードに書き込むデータをカード発行センター１ａの書き込みデータ送信手段１７からネットワーク４を介して書き込みデータ受信手段２１７に於いて受信するか、又は入出力端末２１４から直接データを入力し、一旦制御端末２１ａのハードディスク等の格納手段２１８にそのデータを蓄積した後に、格納手段２１８からカードリーダライタ２２にデータを送りカード媒体２３に書き込むという２段階の工程を経てＩＣカードの発券を行っていた。

しかし、特開２００１－２６６０７６号公開公報及び従来の発券システムに於いてＩＣカードの発券を行う場合、営業拠点は特に路面店等の場合オープンな場所にあることから、固有情報や個人情報を格納している端末の盗難やこれに伴う悪用が発生する可能性があり、又営業拠点で発券処理を手掛けるオペレーターの人数も少ないので相互監視機能が十二分に働かず、営業拠点内での固有情報や個人情報の漏洩のリスクも高いので、顧客に安心して営業拠点に於ける発券システムを利用してもらうことは現状困難であると考えられる。

発明の開示

そこで本発明者は上記問題に鑑み、従来の発券システムのような、書き込みデータを蓄積し、蓄積した書き込みデータをＩＣカードに書き込むという２段階の工程を経ることなく、いかなるセキュリティ環境下の営業拠点に於いても、顧客の安心感とセキュリティを確保し且つリアルタイムで、固有情報や個人情報等を書き込むＩＣカードの発券を可能とするカード発券システム及びカード発券方法を発明した。

請求の範囲１の発明は、

顧客からのＩＣカード申込み依頼に基づいて生成されたカード番号等の固有

情報及び／又は個人情報を含むカード書き込みデータを格納するカード発行センターと、前記カード書き込みデータをネットワークを介して前記カード発行センターから受信し、ＩＣカードに書き込み、ＩＣカードを発券する拠点とにより構築されるカード発券システムに於いて、前記カード発行センターは、前記顧客のカード書き込みデータをネットワークを介して前記拠点に送信するセンター交信手段を有し、前記拠点は、前記センター交信手段から前記カード書き込みデータを受信し、前記拠点の端末内に蓄積することなく前記端末と接続された前記ＩＣカードに転送するカード交信仲介手段を有することにより、前記カード書き込みデータに含まれる固有情報及び／又は個人情報のセキュリティを確保するカード発券システムである。

請求の範囲２の発明は、

顧客からのＩＣカード申込み依頼に基づいて生成されたカード番号等の固有情報及び／又は個人情報を含むカード書き込みデータを格納するカード発行センターにより構築されるカード発券システムに於いて、前記顧客のカード書き込みデータをネットワークを介して拠点に送信し、前記拠点のＩＣカードに前記カード書き込みデータを書き込まれた結果をネットワークを介して前記拠点から受信するセンター交信手段を有し、前記拠点との交信により、確実に前記カード書き込みデータを前記拠点に送信するカード発券システムである。

請求の範囲５の発明は、

顧客のカード番号等の固有情報及び／又は個人情報を含むカード書き込みデータをＩＣカードに書き込み、前記顧客に発券する拠点により構築されるカード発券システムに於いて、前記顧客のカード書き込みデータをネットワークを介してカード発行センターから受信し、前記拠点の端末内に蓄積することなく前記端末と接続された前記ＩＣカードに転送し、前記ＩＣカードに書き込まれた結果をネットワークを介して前記カード発行センターに送信

するカード交信仲介手段を前記端末内に有し、前記カード発行センターとの交信により、確実に前記カード書き込みデータを前記カード発行センターから受信するカード発券システムである。

請求の範囲９の発明は、

顧客からのＩＣカード申込み依頼に基づいて生成されたカード番号等の固有情報及び／又は個人情報を含むカード書き込みデータを格納するカード発行センターと、前記カード書き込みデータをネットワークを介して前記カード発行センターから受信し、ＩＣカードに書き込み、ＩＣカードを発券する拠点とにより実施されるカード発券方法に於いて、前記カード発行センターは、前記顧客のカード書き込みデータをネットワークを介して前記拠点に送信し、前記拠点は、前記カード発行センターから前記カード書き込みデータを受信し、前記拠点の端末内に蓄積することなく前記端末と接続された前記ＩＣカードに転送することにより、前記カード書き込みデータに含まれる固有情報及び／又は個人情報のセキュリティを確保するカード発券方法である。

請求の範囲１０の発明は、

顧客からのＩＣカード申込み依頼に基づいて生成されたカード番号等の固有情報及び／又は個人情報を含むカード書き込みデータを格納するカード発行センターにより実施されるカード発券方法に於いて、前記顧客のカード書き込みデータをネットワークを介して拠点に送信し、前記拠点のＩＣカードに前記カード書き込みデータを書き込まれた結果をネットワークを介して前記拠点から受信し、前記拠点との交信により、確実に前記カード書き込みデータを前記拠点に送信するカード発券方法である。

請求の範囲１３の発明は、

顧客のカード番号等の固有情報及び／又は個人情報を含むカード書き込みデータをＩＣカードに書き込み、前記顧客に発券する拠点により実施されるカード発券方法に於いて、前記顧客のカード書き込みデータをネットワーク

を介してカード発行センターから受信し、前記拠点の端末内に蓄積することなく前記端末と接続された前記ＩＣカードに転送し、前記ＩＣカードに書き込まれた結果をネットワークを介して前記カード発行センターに送信し、前記カード発行センターとの交信により、確実に前記カード書き込みデータを前記カード発行センターから受信するカード発券方法である。

請求の範囲１、２、５、９、１０、１３の発明により、従来の２段階のカード書き込み工程から、カード書き込みデータを端末に蓄積する工程や手段を削除し、拠点でＩＣカードに直接データを書き込むことが出来るようになったので、拠点に於いてカード番号等の固有情報や個人情報のセキュリティを確保し、且つリアルタイムでＩＣカードの発券を行うことが出来る。

請求の範囲３の発明は、

前記カード発行センターから前記拠点に前記カード書き込みデータを送信したという交信結果を格納し、前記カード書き込みデータを受信しＩＣカードに書き込まれた結果を前記拠点から受信し格納するログ管理データベースを前記カード発行センター内に有するカード発券システムである。

請求の範囲１１の発明は、

前記カード発行センターから前記拠点に前記カード書き込みデータを送信したという交信結果を前記カード発行センター内のログ管理データベースに格納し、前記カード書き込みデータを受信しＩＣカードに書き込まれた結果を前記拠点から受信し前記ログ管理データベースに格納するカード発券方法である。

請求の範囲３、１１の発明により、カード発行センターと拠点間の交信結果を管理し、確実にＩＣカードへのデータ書き込みを遂行することが出来る。

請求の範囲４の発明は、

前記拠点の端末から前記カード発行センターへのアクセスの可否を、前記端末に固有の認証情報を格納している制御端末認証データベースから判断する

制御端末認証手段を前記カード発行センター内に有するカード発券システムである。

請求の範囲１２の発明は、

前記拠点の端末から前記カード発行センターへのアクセスの可否を、前記端末に固有の認証情報を格納している制御端末認証データベースから判断するカード発券方法である。

請求の範囲４、１２の発明により、カード発行センターへの不正アクセスを防止し、認証された拠点に於いてのみ、確実にＩＣカードの発券を遂行することが出来る。

請求の範囲６の発明は、

ＩＣカードに前記カード書き込みデータを書き込むカードリーダライタから前記端末へのアクセスの可否を、前記カードリーダライタに固有の認証情報を格納しているリーダライタ認証データベースから判断するリーダライタ認証手段を前記端末内に有するカード発券システムである。

請求の範囲１４の発明は、

ＩＣカードに前記カード書き込みデータを書き込むカードリーダライタから前記端末へのアクセスの可否を、前記カードリーダライタに固有の認証情報を格納しているリーダライタ認証データベースから判断するカード発券方法である。

請求の範囲６、１４の発明により、不正なカードリーダライタの使用を防止し、認証されたカードリーダライタにより確実にＩＣカードの書き込みを遂行することが出来る。

請求の範囲７の発明は、

前記ＩＣカードに内蔵されたアクセス鍵と同じ鍵を用いて、前記ＩＣカードの正規、不正規を判断するカード発券システムである。

請求の範囲１５の発明は、

前記ＩＣカードに内蔵されたアクセス鍵と同じ鍵を用いて、前記ＩＣカードの正規、不正規を判断するカード発券方法である。

請求の範囲７、１５の発明により、不正なＩＣカードへのデータ書き込みを防止し、確実に正規のＩＣカードへの書き込みを遂行することが出来る。

請求の範囲８の発明は、

前記拠点に於いて、顧客への新規ＩＣカード発行又は、発行済みＩＣカード内の個人情報やアプリケーションプログラムの書き換えを行うカード発券システムである。

請求の範囲１６の発明は、

前記拠点に於いて、顧客への新規ＩＣカード発行又は、発行済みＩＣカード内の個人情報やアプリケーションプログラムの書き換えを行うカード発券方法である。

請求の範囲８、１６の発明により、新規のＩＣカード発行のみならず、ＩＣカードの書き換え処理も、拠点に於いてセキュリティを確保し、且つリアルタイムで遂行することが出来る。

符号の説明

１：カード発行センター　１１：センター交信手段　１２：制御端末認証手段　１３：制御端末認証データベース　１４：書き込みデータ暗号手段　１５：暗号鍵データベース　１６：書き込み情報データベース　１７：書き込みデータ送信手段　１８：ログ管理データベース　２：営業拠点　２１：制御端末　２１１：カード交信仲介手段　２１２：暗号復号手段　２１３：鍵情報データベース　２１４：入出力端末　２１５：リーダライタ認証手段　２１６：リーダライタ認証データベース　２１７：書き込みデータ受信手段　２１８：格納手段　２２：カードリーダライタ　２３：カード媒体　３：専用回線　４：ネットワーク

図面の簡単な説明

第１図は本発明のカード発券システムのシステム構成の一例を示す図である。第２図は本発明のカード発券方法のプロセスの流れの一例を示すフローチャート図である。第３図は従来のカード発券システムのシステム構成の一例を示す図である。

発明を実施するための最良の形態

本発明の実施態様の一例を図を用いて詳細に説明する。第１図は本発明のカード発券システムを構成するカード発行センター１と営業拠点２のシステム構成の一例である。

カード発券システムは、高セキュリティ環境下に置かれたカード会社等のサービス提供事業体のカード発行センター１と、比較的低セキュリティ環境下に置かれたサービス提供事業体の営業拠点２との間で、専用回線３を介して通信を行い、顧客に対するＩＣカード（以下、カードと言う）の発券を営業拠点２で行うシステムである。尚、営業拠点２は全国各地に開設された顧客との窓口的役割を果たす拠点であり、サービス提供事業体の支店や子会社も含み、路面店に限らず、デパートや駅構内に設けられた店舗でもよい。

専用回線３は、第三者による漏洩が不可能な電話線等の回線の中でも更に当該サービス事業体用に割り当てられた回線である。専用回線３の使用により、カード発行センター１内で保有している各種情報のセキュリティ確保を行うだけでよく、各所の営業拠点２のセキュリティ環境の是非は問われず、営業拠点２等の各所でのカード発券が可能となる。

以降は専用回線３を使用するものとして説明を行うが、専用回線３の代わりに第三者の漏洩が困難なネットワーク回線や、暗号化技術により第三者による各種情報の解読が不可能なネットワーク回線等を用いてもよい。又、後

述の営業拠点２からカード書き込み結果を受信する為のネットワークとカード発行センター１から営業拠点２にカード書き込みデータを送信する為のネットワークは必ずしも同じ回線を使用する必要はない。

まず、カード発行センター１のシステム構成について説明する。カード発行センター１は、センター交信手段１１、制御端末認証手段１２、制御端末認証データベース１３、書き込みデータ暗号手段１４、暗号鍵データベース１５、書き込み情報データベース１６、ログ管理データベース１８を有する。

センター交信手段１１は、専用回線３を介して営業拠点２の制御端末２１と呼ばれるコンピュータ端末と交信を行う手段である。センター交信手段１１に於いては後述のように、営業拠点２の制御端末２１の認証を行う為のデータ送受信を行ったり、カードに書き込むデータを暗号化したものを営業拠点２に送信したり、営業拠点２からカード書き込み結果を受信する。尚、センター交信手段１１と、制御端末２１内のカード交信仲介手段２１１との交信記録は、逐次カード発行センター１内のログ管理データベース１８に格納される。

制御端末認証手段１２は、営業拠点２の制御端末２１の認証を行う手段である。営業拠点２の制御端末２１にはそれぞれＩＰアドレスが割り当てられ、更に、専用回線３を介してカード発行センター１にアクセスしてきた制御端末２１のみを認証許可することになっている。

制御端末認証データベース１３は、各制御端末２１のＩＰアドレスを格納するデータベースである。万一、制御端末２１自体が盗まれたとしても、専用回線３を介し、且つ特定のＩＰアドレスによってアクセスしないとカード発行センター１から不正アクセスであるとして拒否される。尚、専用回線３は複数回線用意されており、更に常時接続状態である為、複数の営業拠点２からのアクセスにも素早く対応出来る。

書き込みデータ暗号手段１４は、カードの入会申込みや入会申込み内容に

基づいた審査が完了し、カード発券待ち状態となっている顧客のカードに書き込むべき個人情報やカード番号等の固有情報やアプリケーションプログラム等の書き込みデータを書き込み情報データベース１６に格納しておき、営業拠点２からカード発券要求があった場合に書き込みデータを暗号鍵データベース１５に格納されている暗号鍵によって暗号化する手段である。

ここで、個人情報には、氏名等の基本情報の他に、アプリケーションプログラム（例えばクレジット用アプリケーションや、ポイントシステム用アプリケーション）毎に必要となるクレジット支払い設定や与信枠やポイント数等が含まれる。

尚、アプリケーションプログラムは、カード製造工場出荷時に既にカードに書き込まれている場合や、カード製造工場からカード会社のカード発行センター１にカードが納品された後、カード発行センター１で書き込まれ営業拠点２に届けられる場合もある。

次に、営業拠点２のシステム構成について説明する。営業拠点２は、制御端末２１、カードリーダライタ２２を有する。

制御端末２１は、更にカード交信仲介手段２１１、入出力端末２１４、暗号復号手段２１２、鍵情報データベース２１３、リーダライタ認証手段２１５、リーダライタ認証データベース２１６を有するコンピュータ端末である。制御端末２１は従来の制御端末２１ａ（第３図参照）と比較して、格納手段２１８を有さないことが本発明の大きな特徴である。

カード交信仲介手段２１１は、専用回線３を介して制御端末２１毎に固有のＩＰアドレスでカード発行センター１にアクセスする手段である。又、カード交信仲介手段２１１は、カード発行センター１からカードへの書き込みデータを受信し、後述のカードリーダライタ２２に転送してカード発行センター１とカード媒体２３間の仲介を行ったり、入出力端末２１４の内、キーボート等の入力端末を用いてカード発行センター１へのアクセス要求や特定

顧客のカード発券依頼を行ったり、ディスプレイやプリンタ等の出力端末を用いて発券結果出力やカード発行センター１からの指示受信の表示を行う。

暗号復号手段２１２は、カード発行センター１から受信した暗号化済みの書き込みデータを鍵情報データベース２１３内に格納されている復号鍵（カード発行センター１内の暗号鍵データベース１５に格納されている暗号鍵と対の関係にある）によって復号し、カードリーダライタ２２に挿入された、工場出荷状態の、又はカード発行センター１でアプリケーションプログラム等の書き込みデータの一部が書き込まれたカード媒体２３に予め内蔵されているアクセス鍵と同様の、鍵情報データベース２１３に格納されているアクセス鍵を用いてカード媒体２３へのアクセスを可能とした後、一度復号された書き込みデータをカード書き込み用の暗号鍵によって再度暗号化する手段である。

尚、鍵情報データベース２１３及び暗号復号手段２１２はブラックボックス化されており、万一制御端末２１を盗まれたとしても、鍵情報データベース２１３から鍵情報自体を読みとることは困難な仕組みとなっており、制御端末２１には個人情報を蓄積しないので個人情報の流出も不可能である。

更には、後述のカードリーダライタ２２に不正なカードを挿入し、書き込みデータを書き込もうとした場合、鍵情報データベース２１３に格納されているアクセス鍵と同じ鍵を内蔵したカードでないとカードへの書き込みは行えない為、不正なカードからのアクセスはこの時点で拒否され、鍵情報だけがあっても意味がないということになる。

又、この暗号復号手段２１２と鍵情報データベース２１３による暗号化と復号化の処理工程は、営業拠点２の制御端末２１が有している必要は必ずしもなく、カード発行センター１内の書き込みデータ暗号手段１４に於いて最初からカード書き込み用の暗号鍵によって暗号化した書き込みデータを制御端末２１のカード交信仲介手段２１１に送信し、カード発行センター１内の

暗号鍵データベース１５に保有しているアクセス鍵を用いて、カード発行センター１からカード媒体２３にアクセスすることによって、直接カード媒体２３への書き込みを行ってもよい。この場合も、制御端末２１のカード交信仲介手段２１１は単に、カード発行センター１とカード媒体２３間の仲介を行うに過ぎないものである。

リーダライタ認証手段２１５は、後述のカードリーダライタ２２を制御端末２１に接続する際に、カードリーダライタ２２の認証を行う手段である。即ち、不正なカードリーダライタ２２はカードの書き込み及び読みとりに使用出来ない。リーダライタ認証データベース２１６に格納されているカードリーダライタ２２固有の認証情報を元に認証を行い、不正なカードリーダライタ２２とのアクセスは拒否する。

カードリーダライタ２２は、工場出荷状態の、又はカード発行センター１でアプリケーションプログラム等の書き込みデータの一部が書き込まれたカード媒体２３を挿入し、前述のように暗号復号手段２１２によってカード媒体２３へのアクセスを可能とした後、カード交信仲介手段２１１を介してカード発行センター１から受信した書き込みデータをカード媒体２３に直接転送してリアルタイムに書き込む手段であり、予め制御端末２１のリーダライタ認証手段２１５に於いて認証されたカードリーダライタ２２のみが使用可能である。

更にカード媒体２３に書き込みデータが書き込まれたかどうかを、カード媒体２３からカードリーダライタ２２に於いて読みとり、カード交信仲介手段２１１を介してセンター交信手段１１に伝達することにより、あたかもカード発行センター１とカードが直接交信しているのと同じ状態になり、仮に不正なデータが書き込まれたとしてもカード発行センター１で交信結果を随時受信することにより、不正かどうかをチェックすることが出来る。

又、個人情報を含む書き込みデータが営業拠点２に蓄積されることはない

ので、従来のような蓄積、書き込みという２段階の工程を経る必要がなくなり、セキュリティを確保し、且つリアルタイムで営業拠点２に於けるカードの発券が可能となる。尚、カードにデータを書き込んだり、カード内のデータを読みとることが出来る手段があれば、カードリーダライタ２２には限定されない。

次に本発明のプロセスの流れの一例を第２図のフローチャート図及び、第１図のシステム構成図とを用いて詳細に説明する。尚、本実施例については、顧客が営業拠点２に出向き、カードの発券を要求した場合について説明するが、顧客は既に営業拠点２又はカード発行センター１でカード発行の為の入会申込みをＦＡＸや電話や電子メールにより行い、カード発行センター１に於ける審査を経て、顧客に発行するカードに書き込む為の書き込みデータをカード発行センター１内の書き込み情報データベース１６内に格納しているものとする。

営業拠点２の制御端末２１は、カード交信仲介手段２１１により、専用回線３を介してカード発行センター１のセンター交信手段１１にアクセスを要求する（Ｓ２１０）。

センター交信手段１１は制御端末２１からのアクセス要求を受信し、制御端末認証手段１２に於いて、制御端末２１に固有のＩＰアドレスとアクセスしてきた専用回線番号により、制御端末認証データベース１３内に合致するＩＰアドレスがあるかを確認し、制御端末２１のアクセスを許可する（Ｓ２２０）。ＩＰアドレスが異なる、専用回線３を介していない等の不正なアクセスの場合にはアクセスを不許可とし、カード発券が行えないことを通知する（Ｓ３１０）。

アクセスを許可された制御端末２１は、センター交信手段１１に顧客の書き込みデータを要求する旨をカード交信仲介手段２１１から送信する

（Ｓ２３０）。例えば、入出力端末２１４からカード発券対象となる顧客のＩＤやパスワードを入力して送信する。

センター交信手段１１は、カード交信仲介手段２１１に対して、営業拠点２のカードリーダライタ２２を制御端末２１と接続し、カードリーダライタ２２にカードを挿入するよう要求する（Ｓ２４０）。尚、センター交信手段１１とカード交信仲介手段２１１のやりとりは都度、リアルタイムで入出力端末２１４にも表示される。

カード交信仲介手段２１１はカード挿入要求を受信し、制御端末２１にカードリーダライタ２２を接続し、更にカード媒体２３を挿入する（Ｓ２５０）。尚、カードリーダライタ２２は制御端末２１のリーダライタ認証手段２１５により、接続許可を受けている正規のカードリーダライタ２２であるものとする。

挿入されたカード媒体２３とカード発行センター１との間で交信が開始される（Ｓ２６０）。まず、制御端末２１内の暗号復号手段２１は、カード媒体２３に内蔵されているアクセス鍵と同様の鍵情報データベース２１３内のアクセス鍵により、カード媒体２３にアクセスする。不正なカードかどうかは、アクセス鍵自体が存在しなかったり、鍵情報データベース２１３内に格納されているアクセス鍵と異なる鍵がカードに内蔵されていること等から判別することが出来る。不正なカードや、カード内のチップが壊れている等の不良カードである場合は、正規のカードをカードリーダライタ２２に挿入し、再試行する（Ｓ２５５）。

カード交信仲介手段２１１から、カード媒体２３が挿入されたこと、挿入されたカード媒体２３が正規のものであることを受信したセンター交信手段１１は、書き込みデータ暗号手段１４により書き込み情報データベース１６に格納された該当顧客の書き込みデータを暗号化し送信する（Ｓ２７０）。

カード交信仲介手段２１１は、暗号化された書き込みデータを受信し、暗号復号手段２１２に於いてカード発行センター１で暗号化した暗号鍵と対になっている鍵情報データベース２１３内の復号鍵によって書き込みデータを復号し、更にカード媒体２３に書き込みデータを書き込む為に必要な暗号鍵でその書き込みデータを暗号化した後に、カードリーダライタ２２に転送し、挿入されているカード媒体２３に書き込みデータの書き込みを行う（Ｓ２８０）。この時、制御端末２１及びカードリーダライタ２２には書き込みデータの蓄積は行わず、リアルタイムで暗号、復号処理及びカード媒体２３への書き込みを行う。

カードリーダライタ２２への転送結果、カード媒体２３への書き込み可否をカード交信仲介手段２１１からセンター交信手段１１に送信する（Ｓ２９０）。書き込みが行えなかった場合はその旨をセンター交信手段１１に於いて受信し、センター交信手段１１から書き込みデータを再送する等の処置をとる。

尚、センター交信手段１１とカード交信仲介手段２１１との双方の交信結果の履歴は、カード発行センター１側のログ管理データベース１８に逐次格納しておくと望ましい。万一、交信途中で電源が遮断された、アクセス不可能になった等のトラブルが発生した時でも、元の状態に回復させることが可能となる。又、カードに不正なデータが書き込まれた場合は、ログ管理データベース１８内の交信結果からカード発行センター１に於いて判別することが出来る。

書き込み情報データベース１６に、まだ書き込みデータが残っている場合は、前に送信した書き込みデータが確実にカード媒体２３に書き込まれたという結果をカード交信仲介手段２１１から受信したことを先に確認してから、センター交信手段１１から次の書き込みデータをカード交信仲介手段２１１に送信する（Ｓ３００）。尚、最後の書き込みデータであれば、最

後であることが分かるフラグ等を付して書き込みデータとともに送信する。

カード交信仲介手段２１１に於いて受信した書き込みデータは、先のＳ２８０、Ｓ２９０と同様のステップでカード媒体２３への書き込みを行う。又、最後の書き込みデータを受信した時は、再度アクセス鍵を用いてアクセスを終了する等して、カード媒体２３への書き込みを閉じる処理をカードリーダライタ２２側で行い、カード書き込みが正常に終了したことをカード交信仲介手段２１１からセンター交信手段１１に送信する。

別の顧客のカード発券を行う場合は、Ｓ２３０に戻り、同様の手順でカード発行センター１間と制御端末２１間で交信を行う（Ｓ３２０）。

以上のように、営業拠点２の制御端末２１内には書き込みデータを蓄積せず、あくまで制御端末２１は直接カード発行センター１とカード間の仲介の役割を果たすことにより、固有情報や個人情報のセキュリティを確保し且つリアルタイムでカードの発券を行うことが出来るので、空港や鉄道の駅やデパートの窓口等でも、急ぎの顧客向けにカードの発券を行うことが出来るし、カードの発券業務をカード会社以外の業者に委託することも出来る。

又、本発明のカード発券システムでは、本実施例で説明した新規のカード発券以外に、発券済みのカードの書き込みデータ（個人情報やアプリケーションプログラム）の書き換え作業を行うことも可能である。この場合には、カード発行センター１に書き込みデータさえ格納されていれば、顧客が最寄りの営業拠点２に立ち寄るだけで、書き換え作業が完了する。

本発明に於ける各手段、データベースは、その機能が論理的に区別されているのみであって、物理上あるいは事実上は同一の領域を為していてもよい。又データベースの代わりにデータファイルであってもよいことは言うまでもなく、データベースとの記載にはデータファイルをも含んでいる。

尚、本発明を実施するにあたり本実施態様の機能を実現するソフトウェア

のプログラムを記録した記憶媒体をシステムに供給し、そのシステムのコンピュータが記憶媒体に格納されたプログラムを読み出し実行することによっても実現される。

この場合、記憶媒体から読み出されたプログラム自体が前記実施態様の機能を実現することとなり、そのプログラムを記憶した記憶媒体は本発明を構成する。

プログラムを供給するための記憶媒体としては、例えば磁気ディスク、ハードディスク、光ディスク、光磁気ディスク、磁気テープ、不揮発性のメモリカード等を使用することが出来る。

又、コンピュータが読み出したプログラムを実行することにより、上述した実施態様の機能が実現されるだけではなく、そのプログラムの指示に基づき、コンピュータ上で稼働しているオペレーティングシステムなどが実際の処理の一部又は全部を行い、その処理によって前記した実施態様の機能が実現される場合も本発明に含まれる。

産業上の利用可能性

本発明により、いかなるセキュリティ環境下に置かれた各所の営業拠点に於いても、顧客が安心してカード発券を要求することが可能となり、更なるＩＣカードの普及につながる。

顧客の要求に応じて、リアルタイムでＩＣカードを発券することが可能となるので、カード会社の営業拠点のみならず、空港や鉄道の駅やデパートの窓口等でもＩＣカードの発券を行うことが出来る。急ぎの顧客にも便利である。

ＩＣカードに書き込む情報は営業拠点内に蓄積されないので、営業拠点の店員を始め、周囲にいる者や第三者に知られることが絶対になく、カード会社以外の業者がカード発券を代行することも出来る。

新規発券に限らず、既に発行されているＩＣカードに書き込まれている個人情報やアプリケーションプログラムの書き換え、変更を行う際にも本発明は有用であり、カード発行センターに書き込み用データさえ格納されていれば、営業拠点でのカード書き換えが可能となり、わざわざカード発行センターで書き換える必要がないので、時間と輸送コストの削減につながる。

請 求 の 範 囲

1．顧客からのＩＣカード申込み依頼に基づいて生成されたカード番号等の固有情報及び／又は個人情報を含むカード書き込みデータを格納するカード発行センターと、前記カード書き込みデータをネットワークを介して前記カード発行センターから受信し、ＩＣカードに書き込み、ＩＣカードを発券する拠点とにより構築されるカード発券システムに於いて、

前記カード発行センターは、前記顧客のカード書き込みデータをネットワークを介して前記拠点に送信するセンター交信手段を有し、

前記拠点は、前記センター交信手段から前記カード書き込みデータを受信し、前記拠点の端末内に蓄積することなく前記端末と接続された前記ＩＣカードに転送するカード交信仲介手段を有する

ことにより、前記カード書き込みデータに含まれる固有情報及び／又は個人情報のセキュリティを確保する

ことを特徴とするカード発券システム。

2．顧客からのＩＣカード申込み依頼に基づいて生成されたカード番号等の固有情報及び／又は個人情報を含むカード書き込みデータを格納するカード発行センターにより構築されるカード発券システムに於いて、

前記顧客のカード書き込みデータをネットワークを介して拠点に送信し、前記拠点のＩＣカードに前記カード書き込みデータを書き込まれた結果をネットワークを介して前記拠点から受信するセンター交信手段を有し、

前記拠点との交信により、確実に前記カード書き込みデータを前記拠点に送信する

ことを特徴とするカード発券システム。

3．前記カード発券システムは、
前記カード発行センターから前記拠点に前記カード書き込みデータを送信したという交信結果を格納し、
前記カード書き込みデータを受信しＩＣカードに書き込まれた結果を前記拠点から受信し格納するログ管理データベースを前記カード発行センター内に有する
ことを特徴とする請求の範囲１又は請求の範囲２に記載のカード発券システム。

4．前記カード発券システムは、
前記拠点の端末から前記カード発行センターへのアクセスの可否を、前記端末に固有の認証情報を格納している制御端末認証データベースから判断する制御端末認証手段を前記カード発行センター内に有する
ことを特徴とする請求の範囲１から請求の範囲３のいずれかに記載のカード発券システム。

5．顧客のカード番号等の固有情報及び／又は個人情報を含むカード書き込みデータをＩＣカードに書き込み、前記顧客に発券する拠点により構築されるカード発券システムに於いて、
前記顧客のカード書き込みデータをネットワークを介してカード発行センターから受信し、前記拠点の端末内に蓄積することなく前記端末と接続された前記ＩＣカードに転送し、前記ＩＣカードに書き込まれた結果をネットワークを介して前記カード発行センターに送信するカード交信仲介手段を前記端末内に有し、
前記カード発行センターとの交信により、確実に前記カード書き込みデータを前記カード発行センターから受信する

ことを特徴とするカード発券システム。

6．前記カード発券システムは、
ＩＣカードに前記カード書き込みデータを書き込むカードリーダライタから前記端末へのアクセスの可否を、前記カードリーダライタに固有の認証情報を格納しているリーダライタ認証データベースから判断するリーダライタ認証手段を前記端末内に有する
ことを特徴とする請求の範囲１又は請求の範囲５に記載のカード発券システム。

7．前記カード発券システムは、
前記ＩＣカードに内蔵されたアクセス鍵と同じ鍵を用いて、前記ＩＣカードの正規、不正規を判断する
ことを特徴とする請求の範囲１から請求の範囲６のいずれかに記載のカード発券システム。

8．前記カード発券システムは、
前記拠点に於いて、顧客への新規ＩＣカード発行又は、発行済みＩＣカード内の個人情報やアプリケーションプログラムの書き換えを行う
ことを特徴とする請求の範囲１から請求の範囲７のいずれかに記載のカード発券システム。

9．顧客からのＩＣカード申込み依頼に基づいて生成されたカード番号等の固有情報及び／又は個人情報を含むカード書き込みデータを格納するカード発行センターと、前記カード書き込みデータをネットワークを介して前記カード発行センターから受信し、ＩＣカードに書き込み、ＩＣカードを発券

する拠点とにより実施されるカード発券方法に於いて、

前記カード発行センターは、前記顧客のカード書き込みデータをネットワークを介して前記拠点に送信し、

前記拠点は、前記カード発行センターから前記カード書き込みデータを受信し、前記拠点の端末内に蓄積することなく前記端末と接続された前記ＩＣカードに転送する

ことにより、前記カード書き込みデータに含まれる固有情報及び／又は個人情報のセキュリティを確保することを特徴とするカード発券方法。

１０．顧客からのＩＣカード申込み依頼に基づいて生成されたカード番号等の固有情報及び／又は個人情報を含むカード書き込みデータを格納するカード発行センターにより実施されるカード発券方法に於いて、

前記顧客のカード書き込みデータをネットワークを介して拠点に送信し、前記拠点のＩＣカードに前記カード書き込みデータを書き込まれた結果をネットワークを介して前記拠点から受信し、

前記拠点との交信により、確実に前記カード書き込みデータを前記拠点に送信する

ことを特徴とするカード発券方法。

１１．前記カード発券方法は、

前記カード発行センターから前記拠点に前記カード書き込みデータを送信したという交信結果を前記カード発行センター内のログ管理データベースに格納し、

前記カード書き込みデータを受信しＩＣカードに書き込まれた結果を前記拠点から受信し前記ログ管理データベースに格納する

ことを特徴とする請求の範囲９又は請求の範囲１０に記載のカード発券方法。

１２．前記カード発券方法は、
前記拠点の端末から前記カード発行センターへのアクセスの可否を、前記端末に固有の認証情報を格納している制御端末認証データベースから判断することを特徴とする請求の範囲９から請求の範囲１１のいずれかに記載のカード発券方法。

１３．顧客のカード番号等の固有情報及び／又は個人情報を含むカード書き込みデータをＩＣカードに書き込み、前記顧客に発券する拠点により実施されるカード発券方法に於いて、
前記顧客のカード書き込みデータをネットワークを介してカード発行センターから受信し、前記拠点の端末内に蓄積することなく前記端末と接続された前記ＩＣカードに転送し、前記ＩＣカードに書き込まれた結果をネットワークを介して前記カード発行センターに送信し、
前記カード発行センターとの交信により、確実に前記カード書き込みデータを前記カード発行センターから受信する
ことを特徴とするカード発券方法。

１４．前記カード発券方法は、
ＩＣカードに前記カード書き込みデータを書き込むカードリーダライタから前記端末へのアクセスの可否を、前記カードリーダライタに固有の認証情報を格納しているリーダライタ認証データベースから判断する
ことを特徴とする請求の範囲９又は請求の範囲１３に記載のカード発券方法。

１５．前記カード発券方法は、
前記ＩＣカードに内蔵されたアクセス鍵と同じ鍵を用いて、前記ＩＣカードの正規、不正規を判断する

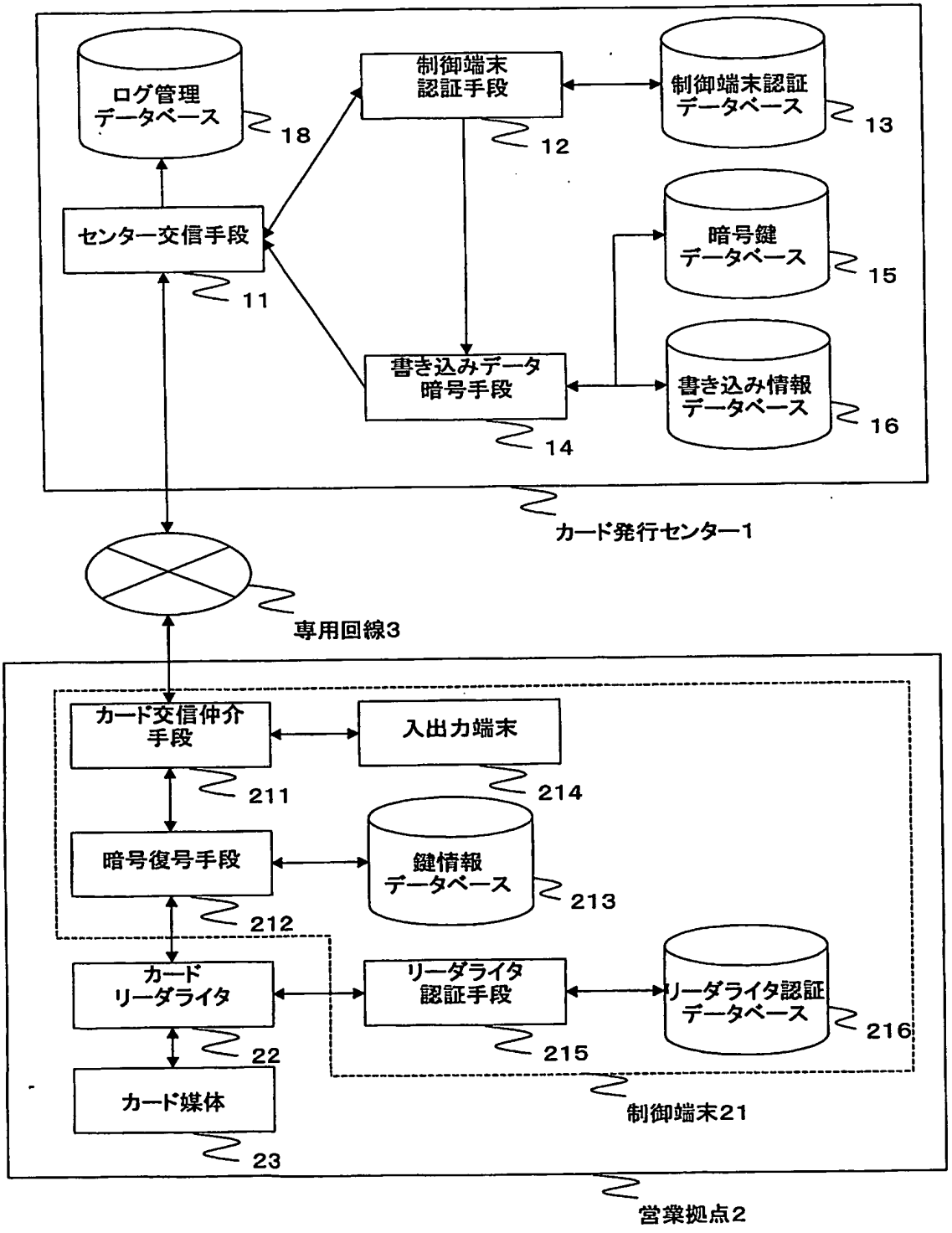
ことを特徴とする請求の範囲９から請求の範囲１４のいずれかに記載のカード発券方法。

１６．前記カード発券方法は、

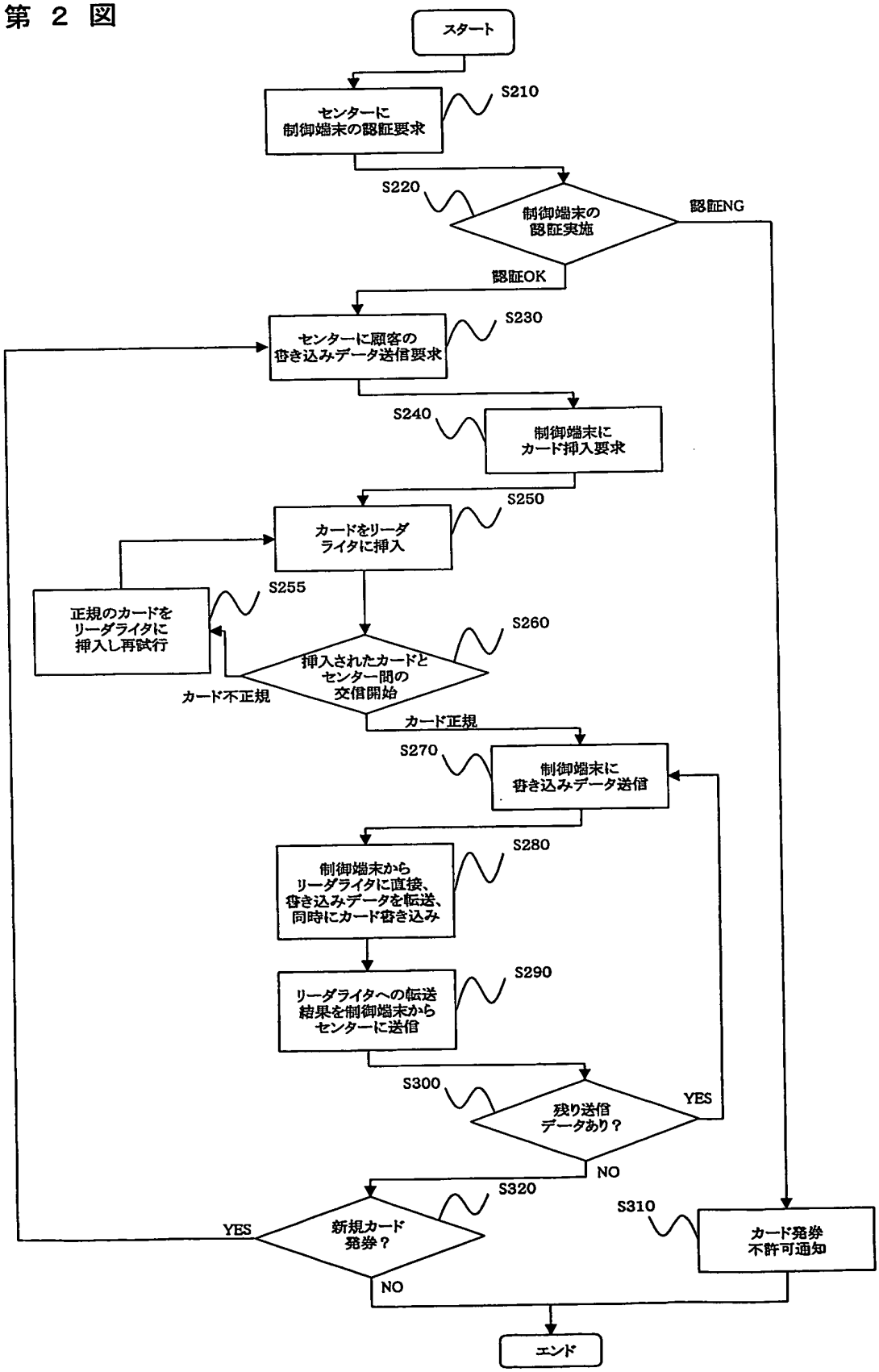
前記拠点に於いて、顧客への新規ＩＣカード発行又は、発行済みＩＣカード内の個人情報やアプリケーションプログラムの書き換えを行う

ことを特徴とする請求の範囲９から請求の範囲１５のいずれかに記載のカード発券方法。

第１図

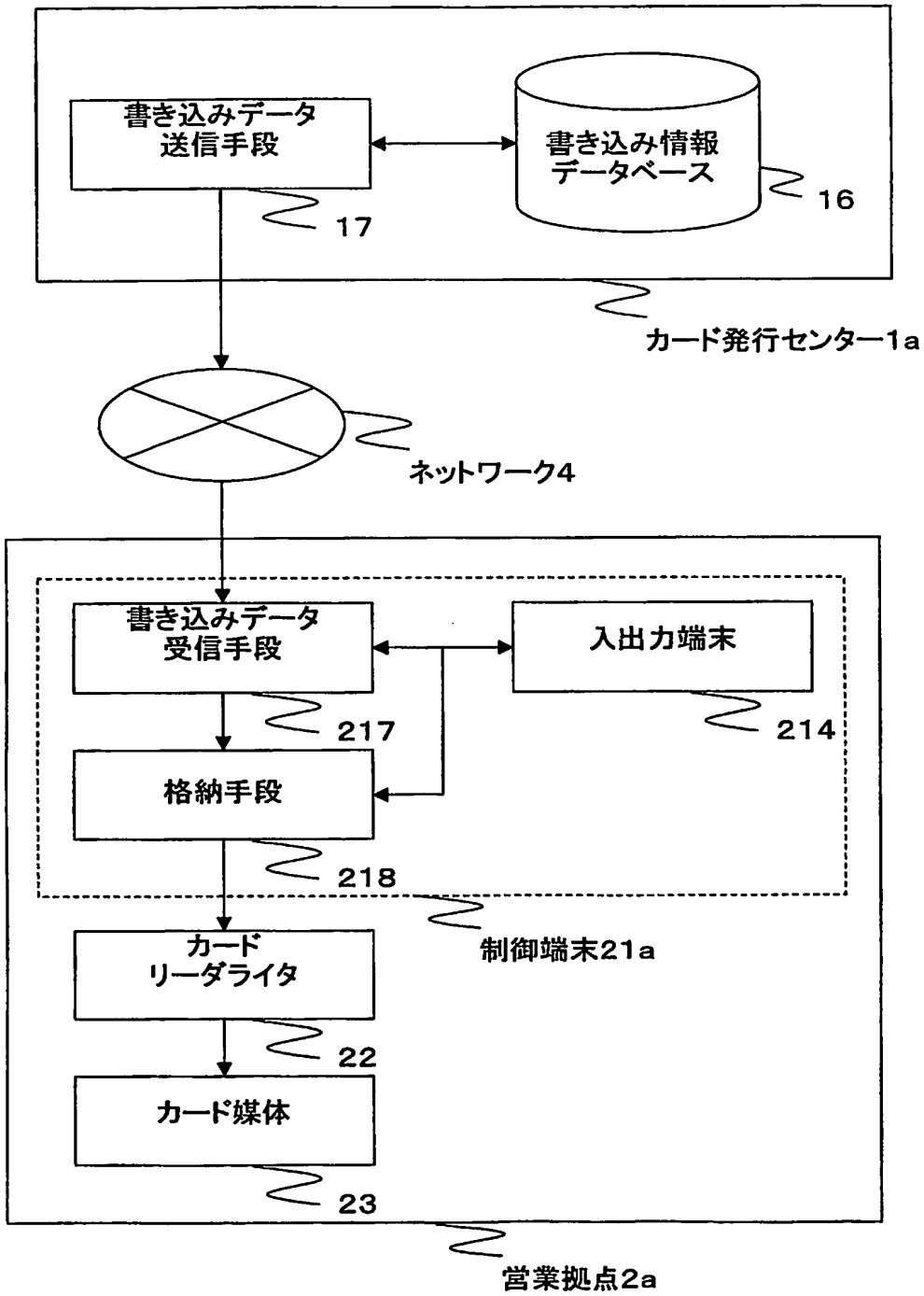

ログ管理
データベース
18
制御端末
認証手段
12
制御端末認証
データベース
13
センター交信手段
11
暗号鍵
データベース
15
書き込みデータ
暗号手段
14
書き込み情報
データベース
16
カード発行センター1
専用回線3
カード交信仲介
手段
211
入出力端末
214
暗号復号手段
212
鍵情報
データベース
213
カード
リーダライタ
22
リーダライタ
認証手段
215
リーダライタ認証
データベース
216
カード媒体
23
制御端末21
営業拠点2

第 2 図



差 替 え 用 紙 (規則26)

第３図


書き込みデータ
送信手段
17
書き込み情報
データベース
16
カード発行センター1a
ネットワーク4
書き込みデータ
受信手段
217
入出力端末
214
格納手段
218
制御端末21a
カード
リーダライタ
22
カード媒体
23
営業拠点2a

特許協力条約に基づく国際出願願書
原本（出願用）- 印刷日時 2003年06月13日（13.06.2003）金曜日 10時11分27秒

VIII-5-1	不利にならない開示又は新規性喪失の例外に関する申立て 不利にならない開示又は新規性喪失の例外に関する申立て（規則4.17(v)及び51の2.1(a)(v)）	本国際出願に関し、 株式会社ジェーシービーは、 本国際出願の請求項に記載された対象が以下のように開示されたことを申し立てる。
VIII-5-1 (i)	開示の種類	その他：プレスリリース
VIII-5-1 (ii)	開示の日付：	2002年06月07日（07.06.2002）
VIII-5-1 (iii)	開示の名称：	
VIII-5-1 (iv)	開示の場所：	
VIII-5-1 (v)	本申立ては、次の指定国のためになされたものである。：	すべての指定国